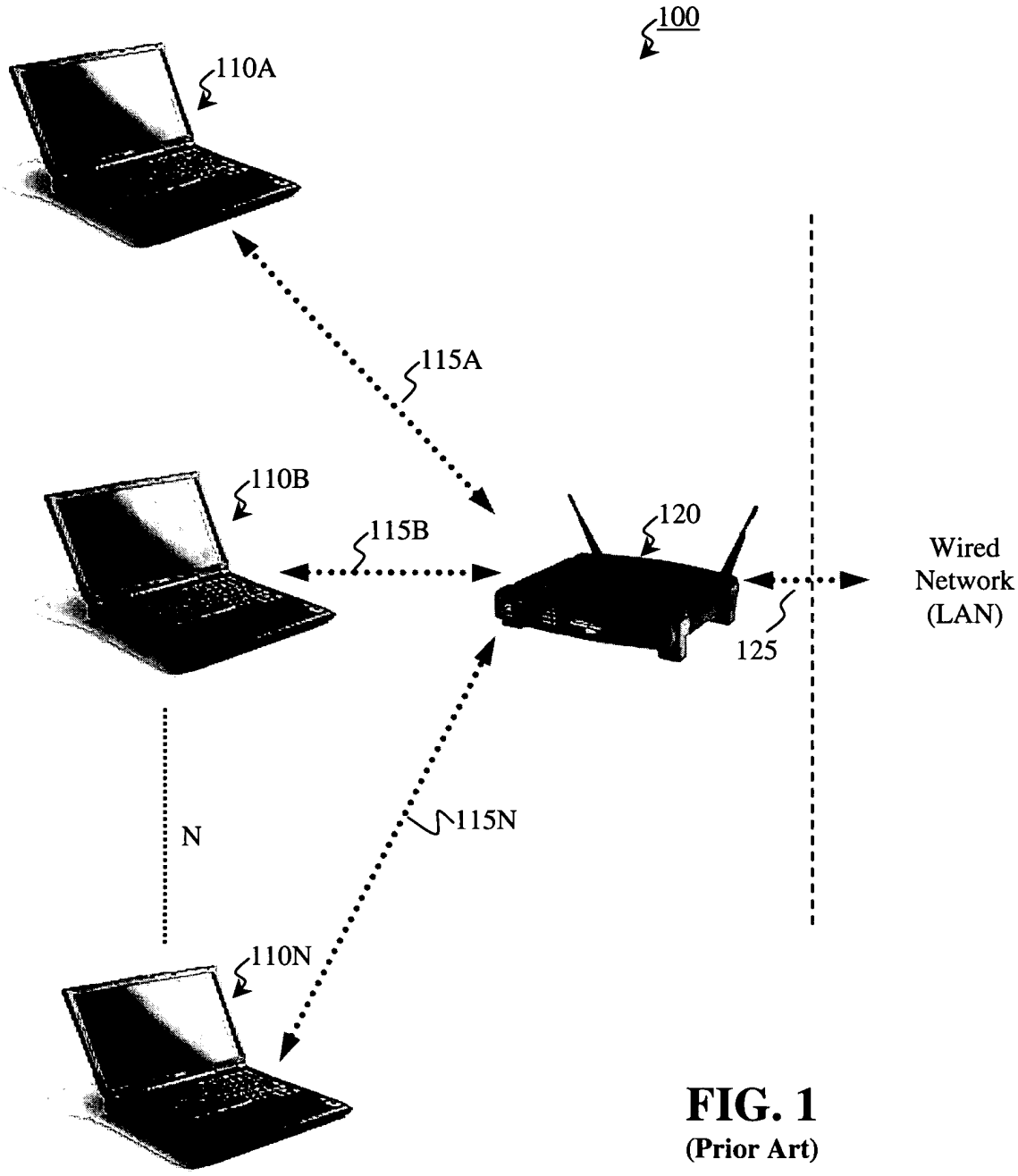


FIG. 1
(Prior Art)

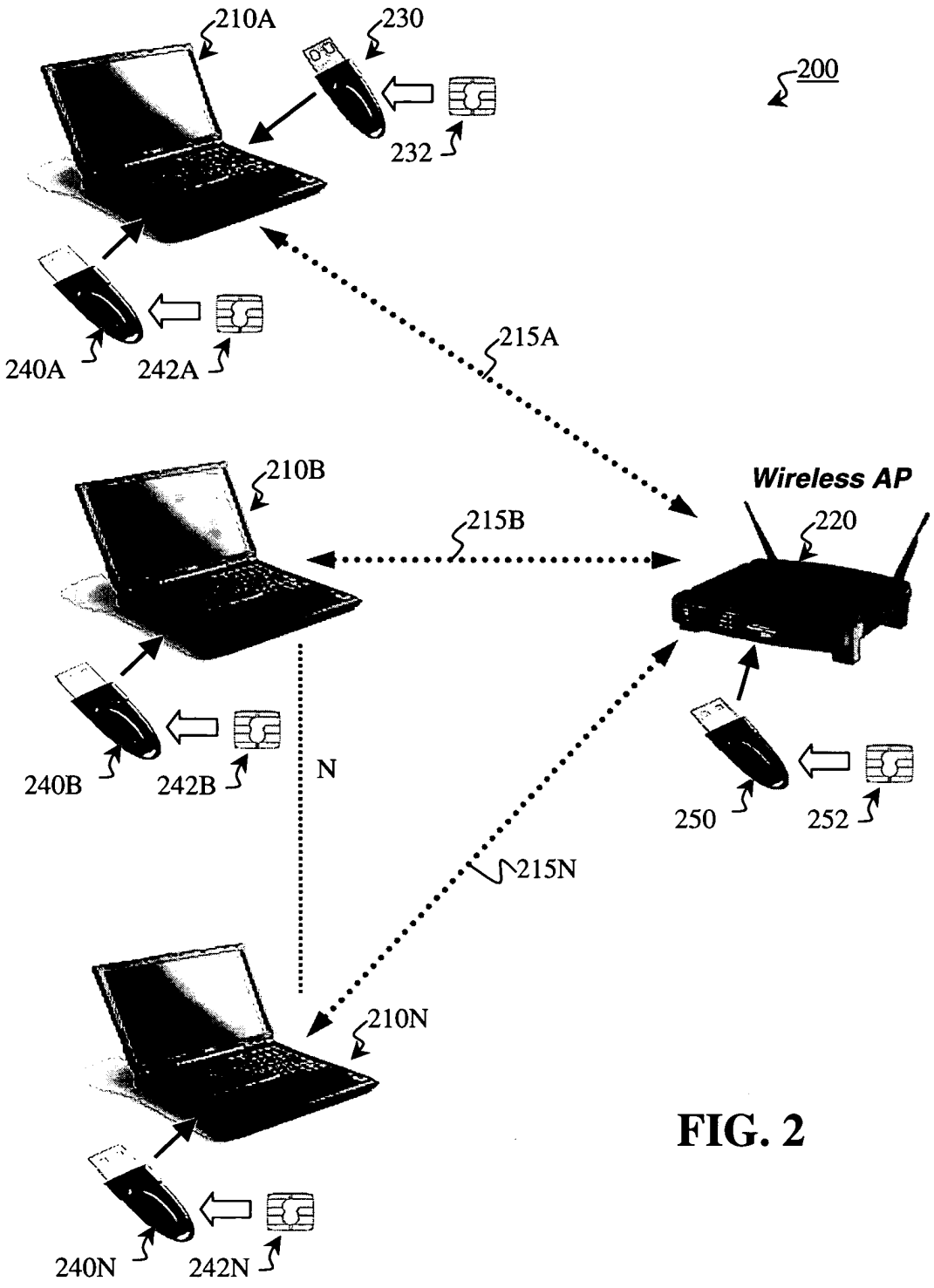
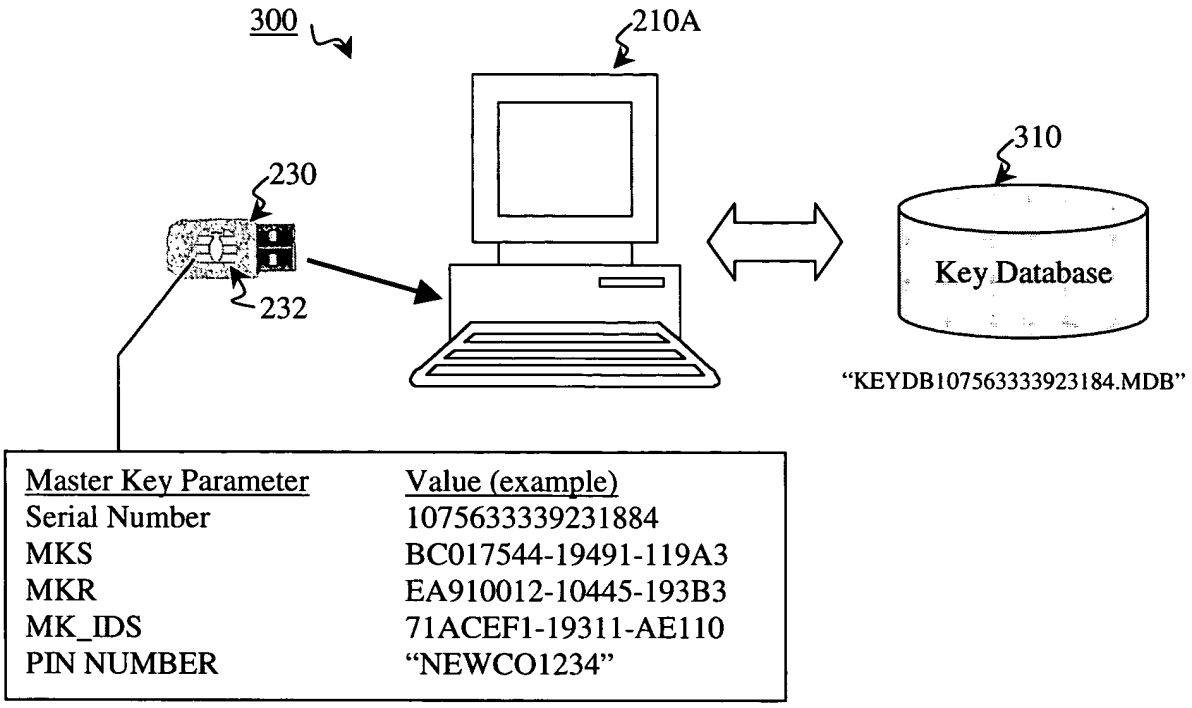

210A
230
200
232
240A
242A
215A
210B
Wireless AP
215B
220
240B
242B
N
250
252
215N
210N
240N
242N

FIG. 2



Master Key Parameter	Value (example)
Serial Number	1075633339231884
MKS	BC017544-19491-119A3
MKR	EA910012-10445-193B3
MK_IDS	71ACEF1-19311-AE110
PIN NUMBER	"NEWCO1234"

FIG. 3

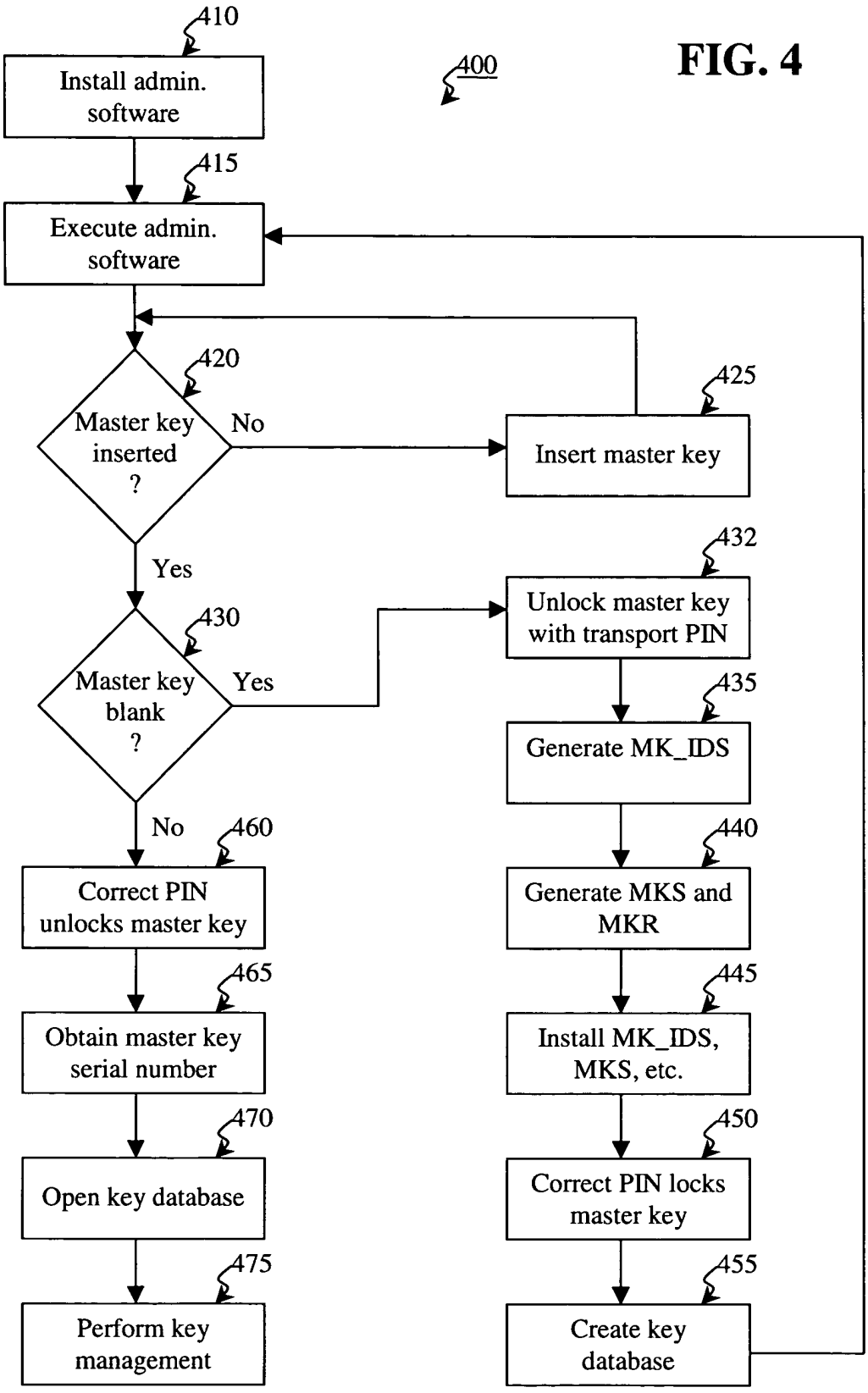
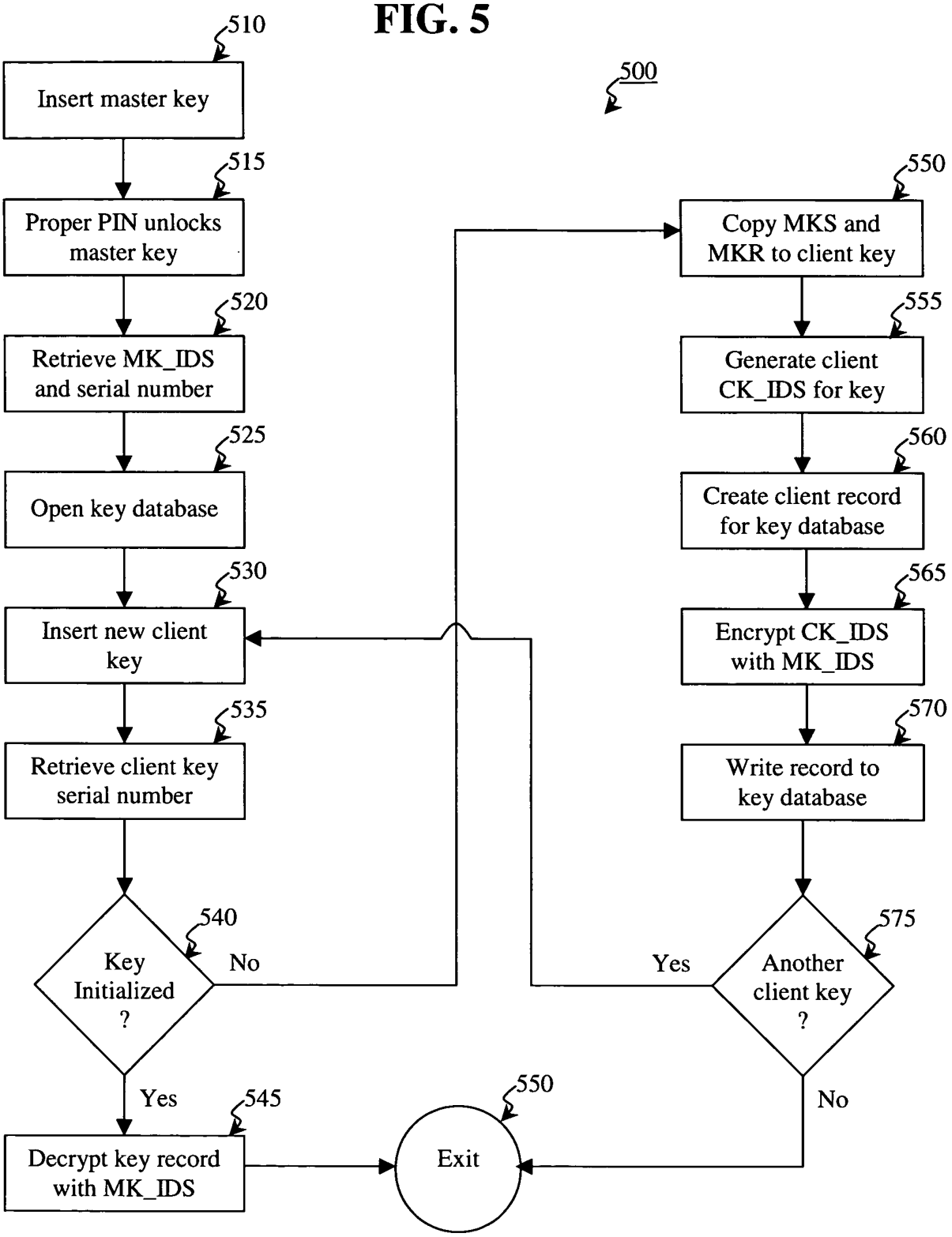

410
Install admin. software
400
415
Execute admin. software
420
Master key inserted ?
No
425
Insert master key
Yes
432
Unlock master key with transport PIN
430
Master key blank ?
Yes
435
Generate MK_IDS
No
460
Correct PIN unlocks master key
440
Generate MKS and MKR
465
Obtain master key serial number
445
Install MK_IDS, MKS, etc.
470
Open key database
450
Correct PIN locks master key
475
Perform key management
455
Create key database

FIG. 4

FIG. 5


500
510
Insert master key
515
Proper PIN unlocks master key
520
Retrieve MK_IDS and serial number
525
Open key database
530
Insert new client key
535
Retrieve client key serial number
540
Key Initialized ?
No
Yes
545
Decrypt key record with MK_IDS
550
Exit
550
Copy MKS and MKR to client key
555
Generate client CK_IDS for key
560
Create client record for key database
565
Encrypt CK_IDS with MK_IDS
570
Write record to key database
575
Another client key ?
Yes
No

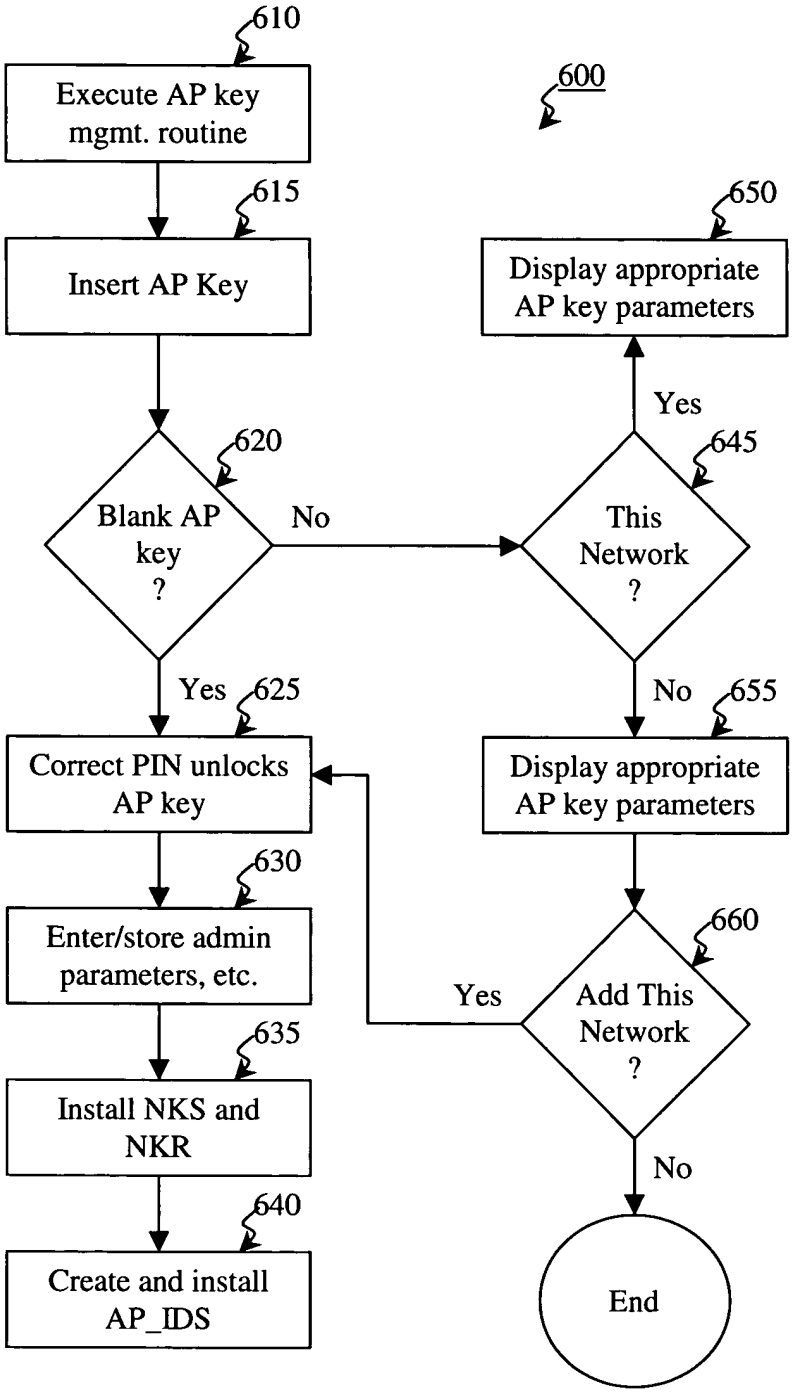
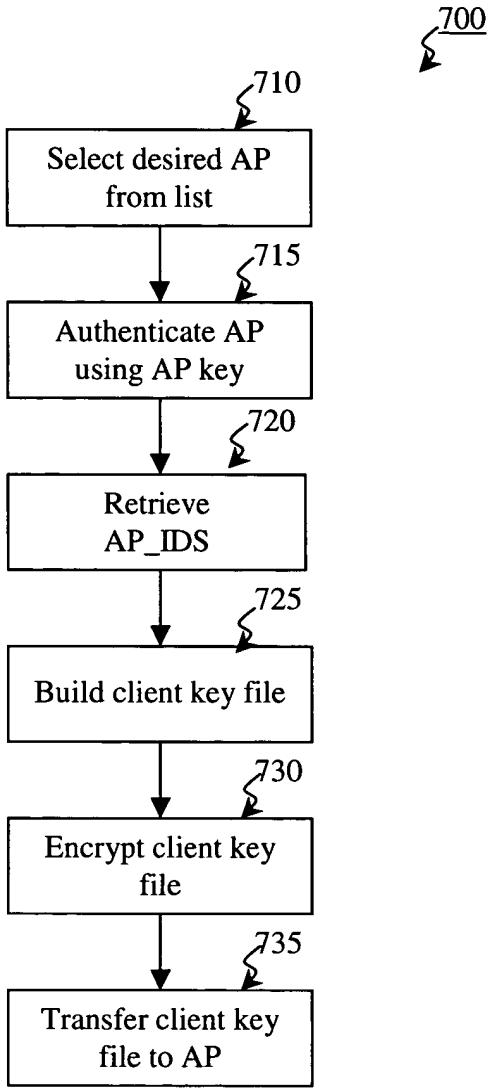

610
Execute AP key mgmt. routine
615
Insert AP Key
620
Blank AP key ?
No
Yes
625
Correct PIN unlocks AP key
630
Enter/store admin parameters, etc.
635
Install NKS and NKR
640
Create and install AP_IDS
600
650
Display appropriate AP key parameters
Yes
645
This Network ?
No
655
Display appropriate AP key parameters
660
Add This Network ?
Yes
No
End

FIG. 6

FIG. 7


700
710
Select desired AP from list
715
Authenticate AP using AP key
720
Retrieve AP_IDS
725
Build client key file
730
Encrypt client key file
735
Transfer client key file to AP

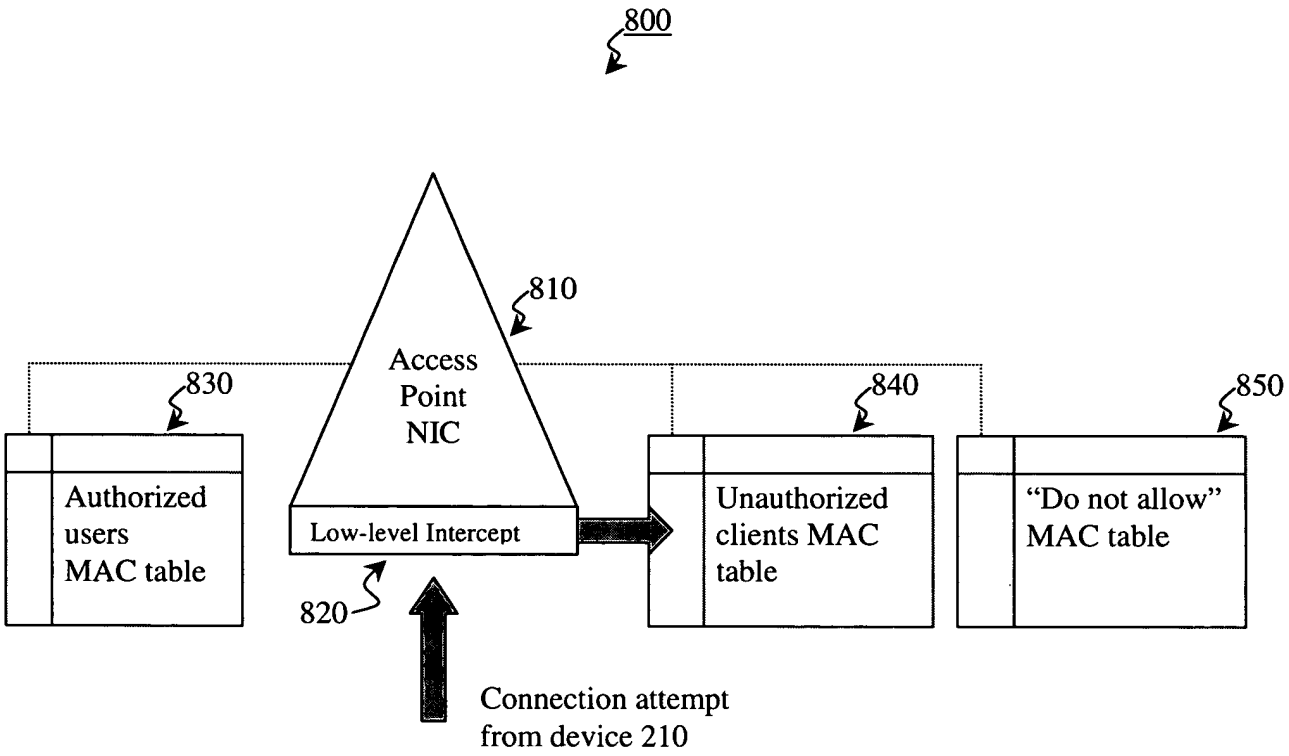
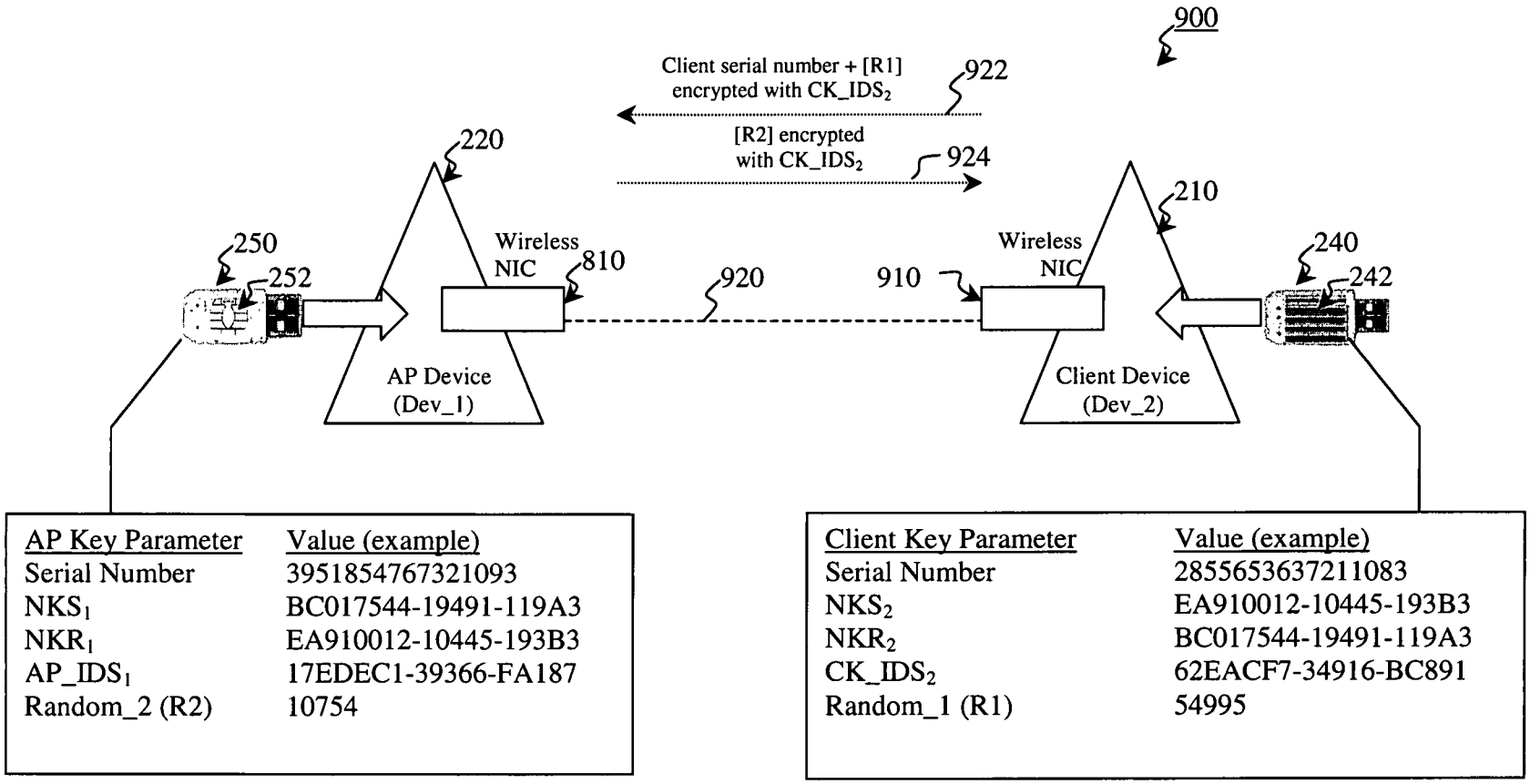

800
810
Access Point NIC
830
840
850
Authorized users MAC table
Low-level Intercept
Unauthorized clients MAC table
"Do not allow" MAC table
820
Connection attempt from device 210

FIG. 8



AP Key Parameter	Value (example)
Serial Number	3951854767321093
NKS_1	BC017544-19491-119A3
NKR_1	EA910012-10445-193B3
AP_IDS_1	17EDEC1-39366-FA187
Random_2 (R2)	10754

Client Key Parameter	Value (example)
Serial Number	2855653637211083
NKS_2	EA910012-10445-193B3
NKR_2	BC017544-19491-119A3
CK_IDS_2	62EACF7-34916-BC891
Random_1 (R1)	54995

FIG. 9A

922

Authentication Request Frame sent to AP

Authentication Algorithm Number	Authentication Transaction Seq. Number	Status Code	Challenge Text	CRC
"3"	"1"	0	Client key serial number, [R1] random number encrypted with CK_IDS_2	

FIG. 9B

924

Authentication Response Frame returned to Client

Authentication Algorithm Number	Authentication Transaction Seq. Number	Status Code	Challenge Text	CRC
"3"	"2"	0	[R2] encrypted with CK_IDS_2	

FIG. 9C

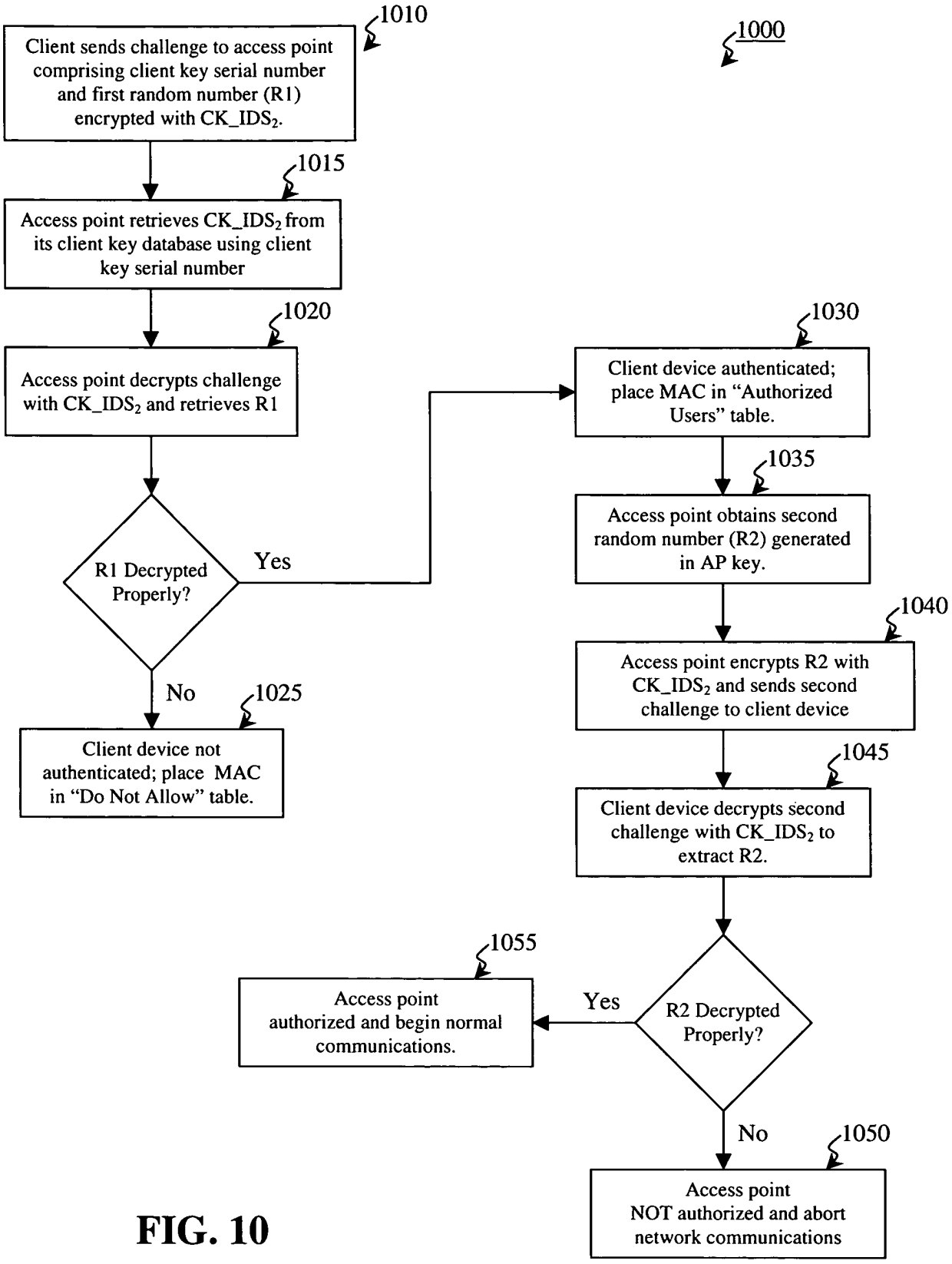

1000
1010
Client sends challenge to access point comprising client key serial number and first random number (R1) encrypted with CK_IDS2.
1015
Access point retrieves CK_IDS2 from its client key database using client key serial number
1020
Access point decrypts challenge with CK_IDS2 and retrieves R1
R1 Decrypted Properly?
Yes
No
1025
Client device not authenticated; place MAC in "Do Not Allow" table.
1030
Client device authenticated; place MAC in "Authorized Users" table.
1035
Access point obtains second random number (R2) generated in AP key.
1040
Access point encrypts R2 with CK_IDS2 and sends second challenge to client device
1045
Client device decrypts second challenge with CK_IDS2 to extract R2.
R2 Decrypted Properly?
Yes
1055
Access point authorized and begin normal communications.
No
1050
Access point NOT authorized and abort network communications

FIG. 10

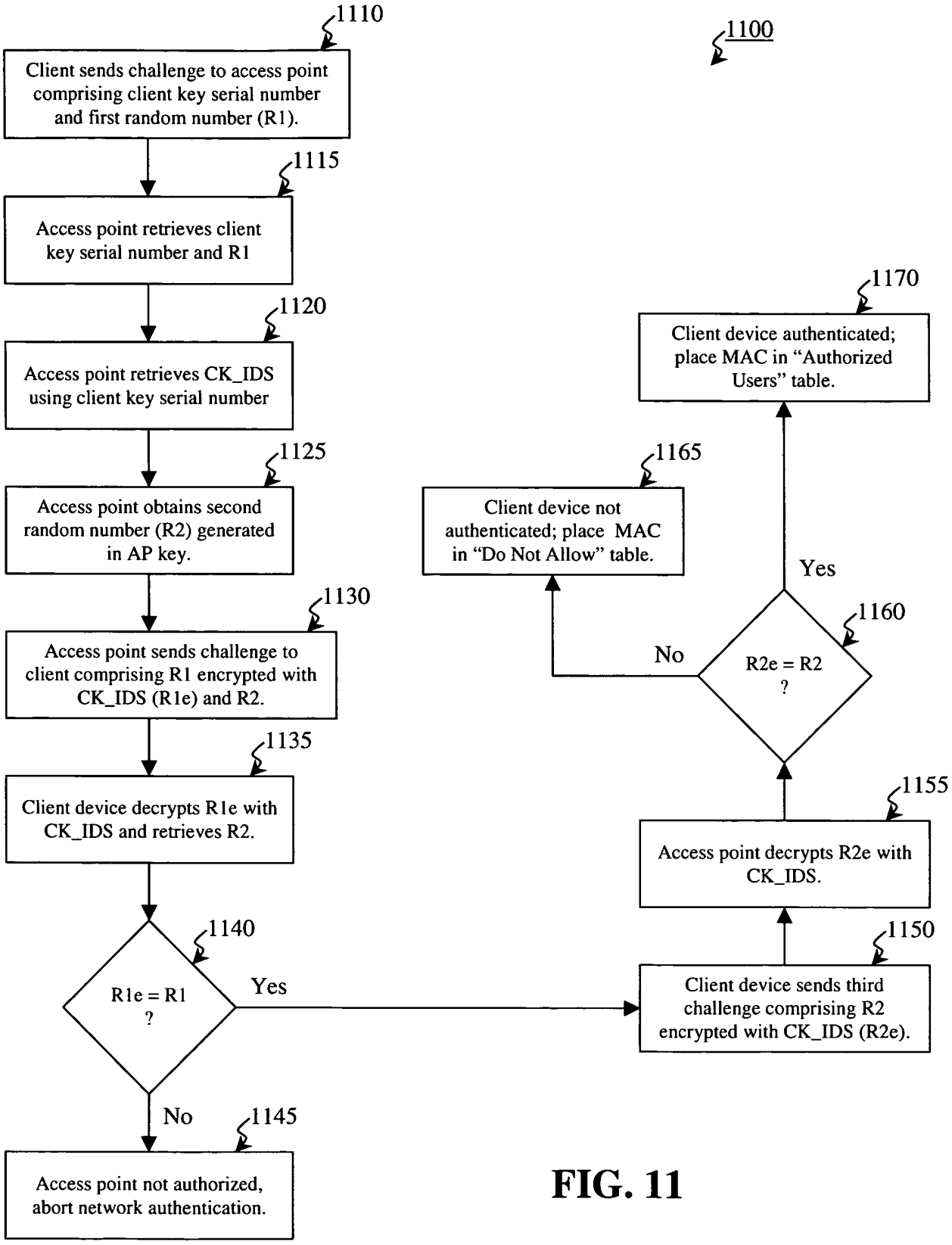
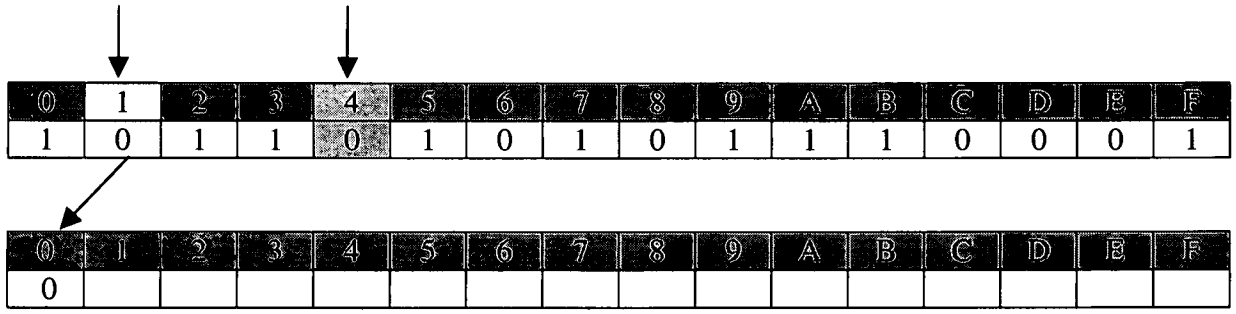

1100
1110
Client sends challenge to access point comprising client key serial number and first random number (R1).
1115
Access point retrieves client key serial number and R1
1120
Access point retrieves CK_IDS using client key serial number
1125
Access point obtains second random number (R2) generated in AP key.
1130
Access point sends challenge to client comprising R1 encrypted with CK_IDS (R1e) and R2.
1135
Client device decrypts R1e with CK_IDS and retrieves R2.
1140
R1e = R1 ?
Yes
No
1145
Access point not authorized, abort network authentication.
1150
Client device sends third challenge comprising R2 encrypted with CK_IDS (R2e).
1155
Access point decrypts R2e with CK_IDS.
1160
R2e = R2 ?
Yes
No
1165
Client device not authenticated; place MAC in "Do Not Allow" table.
1170
Client device authenticated; place MAC in "Authorized Users" table.

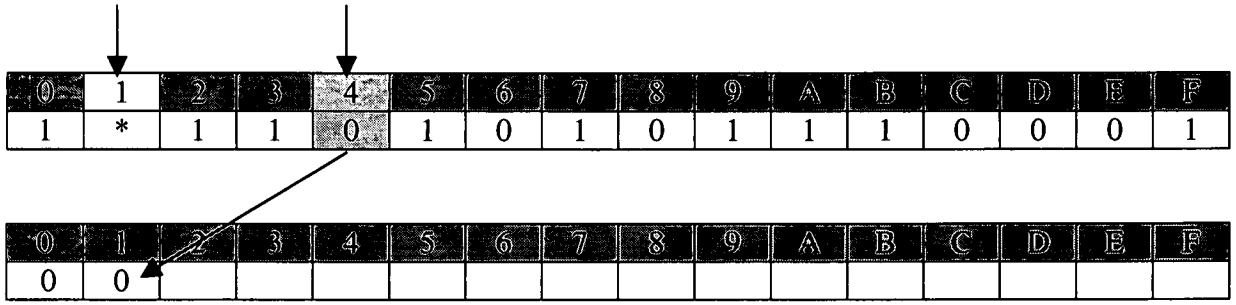
FIG. 11



Original Key

Transposed Key

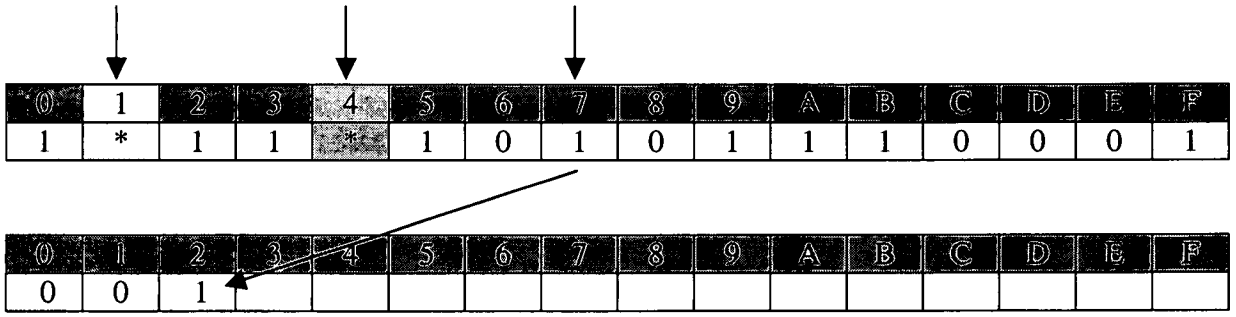
FIG. 12A



Original Key

Transposed Key

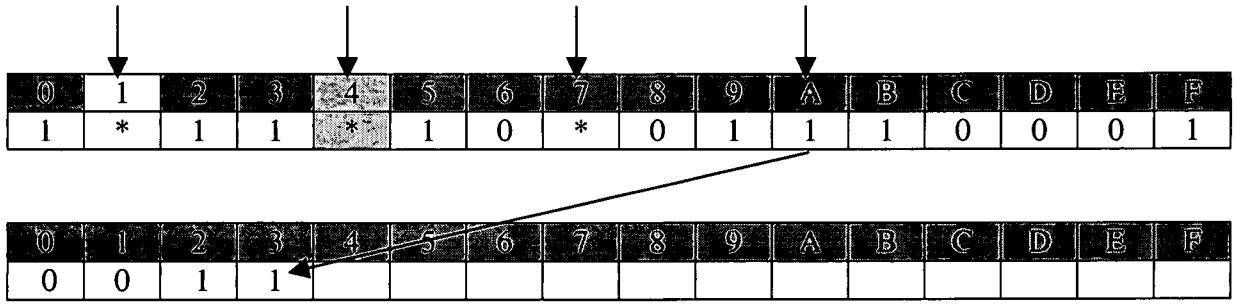
FIG. 12B



Original Key

Transposed Key

FIG. 12C

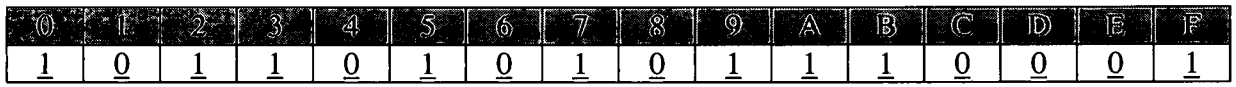


Original Key

Transposed Key

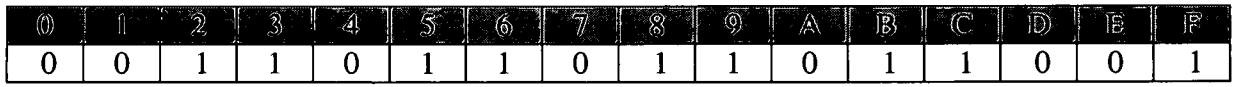
FIG. 12D

Final result



HEX = B571

Original Key



HEX = 36D9

Transposed Key

FIG. 12E